PATENT
Attorney Docket No. COS02007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	**Mail Stop Appeal Brief - Patents**
	)	
Shawn E. WIEDERIN et al.	)	Group Art Unit: 2432
	)	
Application No.: 10/608,137	)	Examiner: B. Lanier
	)	
Filed: June 30, 2003	)	
	)	
For: INTEGRATED SECURITY SYSTEM	)	

U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief - Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314

REPLY BRIEF UNDER 37 C.F.R. § 41.41

This Reply Brief is submitted in response to the Examiner's Answer, dated August 11, 2009.

I. STATUS OF CLAIMS

Claims 1, 4-10, 12-16, and 19-22 are pending in this application. Claims 1, 4-10, 12-16, and 19-22 were rejected in the Office Action dated August 26, 2008 and are the subject of the present appeal. Claims 2, 3, 11, 17, 18, and 23-28 were previously canceled without prejudice or disclaimer. Claims 1, 4-10, 12-16, and 19-22 are reproduced in the Claim Appendix of the Appeal Brief filed January 26, 2009.

II. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 4, 5, 8-10, 12-14, 16, 19, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over SCHNEIER et al. (U.S. Patent Application Publication No. 2002/0087882) in view of JOYCE (U.S. Patent No. 6,519,703).

B. Claims 6, 15, and 21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over SCHNEIER et al. in view of JOYCE and further in view of JUDGE (U.S. Patent No. 6,941,467).

C. Claims 7 and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over SCHNEIER et al. in view of JOYCE and further in view of BATES et al. (U.S. Patent No. 6,785,732).

III. ARGUMENTS

In the "Response to Arguments" section of the Examiner's Answer (pp. 12-13), the Examiner reiterates many of the allegations that are presented in the "Grounds of Rejection" section of the Examiner's Answer and the Office Action, dated August 26, 2008. Thus, Appellants' arguments presented in the Appeal Brief, filed January 26, 2009, are applicable to those allegations. Appellants submit the following additional remarks.

A. Claims 1, 4, 5, 8, and 9

In the Appeal Brief, Appellants demonstrated that SCHNEIER et al. and JOYCE, whether taken alone or in any reasonable combination, do not disclose or suggest forwarding logic configured to forward report information to a remote central management system when the report information indicates that first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device, as recited in claim 1 (see pp. 12-16 of the Appeal Brief). In response, the Examiner alleges that "the SOC of Schneier is relied upon to teach the claimed remote central management system. Since the SOC informs the network response subsystem of which IP address to not allow (i.e. block) access to the customer's network, the SOC effectively makes a forwarding decision on behalf of the sentry system" (Examiner's Answer, p. 13). Appellants respectfully disagree with the Examiner's allegation.

SCHNEIER et al. discloses forwarding residue information that may be worthy of additional analysis to gateway system 4000 within the SOC (paragraph 0065). Gateway messages arrive at SOCRATES, within the SOC, from the gateway system, where event records

are stored and linked with other even records to form "problem tickets," which are then opened and displayed on security analyst consoles for handling by security analysts (paragraph 0085).

Therefore, SCHNEIER et al. discloses that, when possibly interesting information is selected, the information is matched with other information and displayed on security analyst consoles. Assuming, for the sake of argument, that the interesting information of SCHNEIER et al. can reasonably be construed as the first data of claim 1 and that the SOC can reasonably be construed as the remote central management system of claim 1 (points with which Appellants do not agree), SCHNEIER et al. does not disclose forwarding logic configured to forward report information to the SOC when the report information indicates that the interesting information potentially contains malicious content, the report information allowing the SOC to make a forwarding decision on behalf of the device, as would be required by SCHNEIER et al. based on the Examiner's interpretation of claim 1. Instead, as noted above, at the SOC, problem tickets are formed for handling by security analysts. Because SCHNEIER et al. discloses a probe/sentry system that monitors and collects information concerning the status of a network and its components (paragraph 0035), there would be no reason for the sentry system of SCHNEIER et al. to make forwarding decisions. Therefore, this section of SCHNEIER et al. does not disclose or suggest forwarding logic configured to forward report information to a remote central management system when the report information indicates that first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device, as recited in claim 1.

Furthermore, as noted by the Examiner, SCHNEIER et al. discloses that the SOC might request that the network response subsystem not allow a certain IP address to access the

customer's network for a period of time (paragraph 0068). This section of SCHNEIER et al. deals with blocking a certain IP address from accessing a customer's network. This section of SCHNEIER et al. has nothing to do with making a forwarding decision. Even assuming, for the sake of argument, that the SOC of SCHNEIER et al. can be construed as corresponding to the remote central management system and that blocking a certain IP address can be construed as making a forwarding decision (points with which Appellants do not agree), SCHNEIER et al. does not disclose forwarding logic configured to forward report information to the SOC when the report information indicates that the interesting information potentially contains malicious content, the report information allowing the SOC to block a certain IP address on behalf of the device, as would be required by SCHNEIER et al. based on the Examiner's interpretation of claim 1. In fact, SCHNEIER et al. does not disclose that blocking the IP address is based on report information forwarded to the SOC at all. Therefore, SCHNEIER et al. does not disclose or suggest forwarding logic configured to forward report information to a remote central management system when the report information indicates that first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device, as recited in claim 1.

The disclosure of JOYCE does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above.

For at least the reasons given above and for those reasons given in the Appeal Brief, Appellants respectfully submit that the rejection of claims 1, 4, 5, 8, and 9 under 35 U.S.C. § 103(a) based on SCHNEIER et al. and JOYCE is improper. Accordingly, Appellants request that the rejection of claims 1, 4, 5, 8, and 9 be reversed.

The Examiner's allegations with respect to the claims not addressed herein are reiterations of the arguments set forth in the Office Action and have been addressed in the Appeal brief at pages 12-23.

IV. CONCLUSION

In view of the foregoing arguments and those arguments presented in the Appeal Brief, Appellants respectfully solicit the Honorable Board to reverse the Examiner's rejections of claims 1, 4-10, 12-16, and 19-22.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY & HARRITY, LLP

By: /Meagan S. Walling, Reg. No. 60,112/
Meagan S. Walling
Reg. No. 60,112

Date: October 7, 2009
11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800 main
(571) 432-0841 direct